

AD-AU44 439

ROCHESTER UNIV NY DEPT OF COMPUTER SCIENCE  
ON THE N(LOG2N) ISOMORPHISM TECHNIQUE, (U)  
MAR 77 G L MILLER

TR-17

UNCLASSIFIED

F/G 12/1

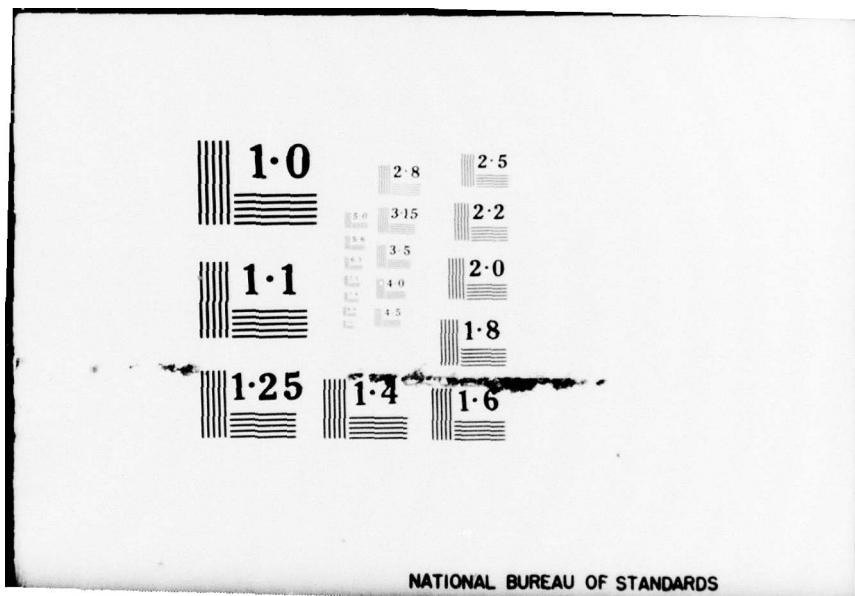
NU0014-75-C-1091

NL

1 OF 1  
ADA  
044439



END  
DATE  
FILED  
10-77  
DDC



NATIONAL BUREAU OF STANDARDS

AD No.

DDC FILE COPY

AD A 044439

计算  
机  
科  
学

11  
B 51

DDC  
REF ID: A  
SEP 22 1977  
R  
A

theCSRG

Department of Computer Science  
University of Rochester  
Rochester, New York 14627

DISTRIBUTION STATEMENT A  
Approved for public release;  
Distribution Unlimited

6 On the  $n^{\log_2 n}$  Isomorphism Technique\*

10 Gary L. Miller  
Departments of Computer Science  
and Mathematics  
The University of Rochester

14 TR17

11 MARCH 1977

12 10 P.M.

D D C  
RECEIVED  
SEP 22 1977  
RESULTS  
A

Tarjan has given an algorithm for deciding isomorphism of two groups of order  $n$  (given as multiplication tables) which runs in  $O(n^{\log_2 n} + O(1))$  steps where  $n$  is the order of the groups. Tarjan uses the fact that a group of  $n$  is generated by  $\log n$  elements. In this paper, we show that Tarjan technique generalizes to isomorphism of quasigroups, latin squares, and some graphs generated from latin squares.

DISTRIBUTION STATEMENT A  
Approved for public release;  
Distribution Unlimited

\*This research was in part supported by the National Research Council, Grant #NRC-A5549; in part by the Alfred P. Sloan Foundation under Grant #74-12-5; and in part by the Advanced Research Projects Agency of the Dept. of Defense, monitored by ONR under Contract #N00014-75-C-1091.

NRC-A5549 410386 ✓

A group throughout this paper is a Caley table. If  $G$  is a group of order  $n$  and we pick some linear ordering of  $G$  we can then view  $G$  as a binary function on  $\{1, \dots, n\}$  and the Caley table as a  $n \times n$  matrix consisting of integers between 1 and  $n$ . In fact this table is a latin square (every number between 1 and  $n$  appears exactly once in every row and in every column). On the other hand, latin squares can be viewed as binary functions; whereas functions whose multiplication tables are latin squares are called quasigroups.

Giving the definition once more we have: A group is a binary operation  $*$  satisfying 1) and 2).

- 1) a)  $\exists!x(a * b = x)$
- b)  $\exists!x(a * x = b)$
- c)  $\exists!x(x * a = b)$
- 2)  $(a * b) * c = a * (b * c)$

A quasigroup is a binary operation satisfying 1), and a quasigroup viewed as a table or a trinary relation is a latin square.

For groups or functions it is clear what we mean by isomorphism, namely,  $G$  is isomorphic to  $G'$  if there exists a 1-1 onto function  $g$  from  $G$  to  $G'$  such that  $g(x * y) = g(x) *' g(y)$ . If we view  $G$  and  $G'$  as trinary relations  $< , , >$  and  $< , , >'$  respectively, then we get  $<x, y, z> \in G$  implies  $<g(x), g(y), g(z)> \in G'$ . Thus, viewing latin squares as quasigroups we say  $L$  and  $L'$  are isomorphic if there exists a permutation  $\sigma$  such that if we simultaneously interchange rows, columns, and values in  $L$  we get  $L'$ . But this definition is quite restrictive. We know that independently permuting rows, columns, and values preserves the latin

SEARCHED   
INDEXED   
SERIALIZED   
FILED

SEARCHED   
INDEXED   
SERIALIZED   
FILED

LIBRARY COPIES  
AVAIL. REG. OR SPECIAL

A

square properties. Thus, we say two latin squares are isotopic if we can get from one to the other by independently permuting rows, columns, and values; see [ 1 ].

Definition: Two latin squares  $L$  and  $L'$  are said to be isotopic if there exists permutations  $(\alpha, \beta, \gamma)$  such that  $\langle x, y, z \rangle \in L$  implies  $\langle \alpha(x), \beta(y), \gamma(z) \rangle' \in L'$ , which is denoted by  $L \equiv L'$ .

We say that two latin squares  $L$  and  $L'$  are conjugate if there exists a permutation  $\alpha \in S_3$  such that  $\langle x_1, x_2, x_3 \rangle \in L$  implies  $\langle x_{\alpha(1)}, x_{\alpha(2)}, x_{\alpha(3)} \rangle' \in L'$ . Finally,  $L$  and  $L'$  are main class isotopic, denoted by  $L \equiv_M L'$ , if we can get from  $L$  to  $L'$  by a conjugation and an isotopic map.

Tarjan [ 2 ] observed that since groups of order  $n$  are generated by a set of elements of size at most  $\log_2 n$ , group isomorphism can be done in  $O(n^{\log_2 n} + O(1))$  steps. Lipton, Snyder, and Zalcstein [ 3 ], independently of Tarjan, showed a stronger result; namely, group isomorphism can be solved in  $O(\log^2 n)$  space. The  $O(\log^2 n)$  result seems to be dependent on the fact that groups are associative while the  $O(n^{\log_2 n} + O(1))$  result generalizes to quasigroups:

Theorem 1: Quasigroup isomorphism can be solved in  $O(n^{\log_2 n} + O(1))$  steps.

Proof: Property 1a) says the binary operation is a well-defined function. Now, 1b) and 1c) give two other well-defined functions associated with a quasigroup. We shall say that a set of elements generates the quasigroup if their closure under these three functions is the whole quasigroup.

Thus, using this definition, we prove a generalization of the observation about the size of the minimal generator set.

Lemma 1: A quasigroup is generated by a set containing at most  $\log_2 n$  elements.

Proof: To prove the lemma we need only prove that if  $H$  is a proper sub-quasigroup of  $G$  then  $|G| \geq 2|H|$ . Pick  $b \in G-H$ . Consider the elements  $H \cdot b$ . Now, all the products are distinct, for if  $h \cdot b = h' \cdot b$  where  $h, h' \in H$  then  $h = h'$  by property 1c). Secondly,  $H \cdot b$  is disjoint from  $H$  for if  $h = h' \cdot b$  when  $h, h' \in H$  then  $b \in H$  by property 1b). This contradicts the fact that  $b \notin H$ . Thus,  $H \cdot b \subseteq G-H$  and  $|H \cdot b| = |H|$  which proves the lemma.

To finish the proof of Theorem 1 we give a short description of the algorithm with two quasigroups,  $G$  and  $G'$ , as input:

- 1) Find a set of generators for  $G$ , containing at most  $\log_2 n$  elements, say  $a_1, \dots, a_m$ .
- 2) For each set of  $m$  elements in  $G'$ , say,  $\{b_1, \dots, b_m\}$  check to see if the map induced by  $a_i \rightarrow b_i$ ,  $1 \leq i \leq m$  is a well-defined isomorphism of  $G$  onto  $G'$ .
- 3) If a set of  $m$  elements of  $G'$  is found in 2) accept; otherwise reject.

Now consider isotopic latin squares. Using isotopic maps we can always put the latin square in a "normal" form; namely, the first row and first column are the sequence  $1, 2, \dots, n$ . This normal form is not unique. In fact, it is not unique up to isomorphism, but is almost

unique up to isomorphism. Suppose that  $L$  and  $L'$  are two isotopic latin squares in normal form and  $(\alpha, \beta, \gamma)$  is the isotopic map from  $L$  to  $L'$ .

Given a permutation  $\alpha$ , let  $\alpha^{(1)}$  be the transposition  $(1, \alpha^{-1}(1))$ . Now the decomposition of  $\alpha$  into  $(\alpha\alpha^{(1)})(\alpha^{(1)})$  splits  $\alpha$  into  $\alpha^{(1)}$  which may move 1 while  $\alpha\alpha^{(1)}$  leaves 1 fixed. The following result simply says that up to choosing who gets to be the identity  $L$  and  $L'$  are isomorphic.

Lemma 2: Given two latin squares  $L$  and  $L'$  in normal form which are isotopic by the permutations  $\langle \alpha, \beta, \gamma \rangle$  then  $\langle \alpha^{(1)}, \beta^{(1)}, \gamma^{(1)} \rangle(L)$  is isomorphic to  $L'$ .

Proof: Now,  $\langle \alpha^{(1)}, \beta^{(1)}, \gamma^{(1)} \rangle(L) = L''$  is still isotopic to  $L'$  by  $\langle \alpha' = \alpha \cdot \alpha^{(1)}, \beta' = \beta \cdot \beta^{(1)}, \gamma' = \gamma \cdot \gamma^{(1)} \rangle$ , and  $L''$  is in normal form. We shall show that in fact  $\alpha' = \beta' = \gamma'$ . Suppose that  $\gamma'(V) = W$ .  $\gamma'$  has changed the  $V$  in column  $V$  to a  $W$ . Thus,  $\beta'$  must move column  $V$  to column  $W$  to insure that the latin square is in normal form. Similarly,  $\alpha'$  must move row  $V$  to row  $W$ . Therefore  $\alpha' = \beta' = \gamma'$  and the lemma is proved.

Theorem 2: Isotopy of latin squares is decidable in  $O(n \log_2 n + O(1))$  time.

Proof: The algorithm, on input  $L$  and  $L'$ , arbitrarily puts  $L'$  in normal form and then for each of the  $n^2$  possible candidates for the identity it puts  $L$  in normal form. Now the algorithm checks if any of these  $n^2$  normal forms of  $L$  are in fact isomorphic to  $L'$ .

Since there are only six ways to conjugate latin squares, we get that main class isotopy is in time  $O(n \log_2 n + O(1))$ .

Corollary: Main class isotopy of latin squares is decidable in  $O(n \log_2 n + O(1))$  time.

A natural graph associated with a latin square is called a latin square graph which is defined as follows:

Definition: Given a latin square, say  $L (\ell_{ij})$ , of size  $n$ , then the latin square graph associated with  $L$ , say  $G(L)$ , has  $n^2$  nodes  $g_{ij}$ ,  $1 \leq i, j \leq n$ ; and the nodes  $g_{ij}$  and  $g_{kl}$  are connected if one of the following holds:

- 1)  $i = k$
- 2)  $j = l$
- 3)  $\ell_{ij} = \ell_{kl}$

Latin square graphs consist of  $3n$   $n$ -cliques ( $n$  row cliques,  $n$  column cliques, and  $n$  value cliques). Two  $n$ -cliques are disjoint iff they are either different row, different column, or different value cliques.

Thus we get the following result:

Lemma 3: If  $L$  and  $L'$  are latin squares, and  $G(L)$  and  $G(L')$  are latin square graphs, then  $L$  is main class isotopic to  $L'$  iff  $G(L)$  is isomorphic to  $G(L')$ .

If we now give an efficient method of retrieving the latin square from the latin square graph we will have a  $O(n \log_2 n + O(1))$  algorithm for latin square graph isomorphism; namely, retrieve the two latin squares and check the two latin squares for main class isotopy.

Lemma 4: In  $O(n^3)$  steps we can retrieve the latin square from the latin square graph where  $n$  is the dimension of the latin square.

Proof: Let  $G$  be a latin square graph on  $n^2$  nodes. To construct a latin square we shall associate each node of  $G$  with an element in a  $n \times n$  matrix  $A(a_{ij})$  and also assign a value to the nodes or elements.

Algorithm:

- 1) Pick two connected nodes, say  $x_1$  and  $x_2$ .
- 2) Find the  $n$  nodes common to  $x_1$  and  $x_2$ . Now,  $n-2$  of the nodes are connected to each other, say  $x_3, \dots, x_n$ .  
Let  $y_2$  be one of the nodes that is not connected to  $x_3, \dots, x_n$ .
- 3) Associate  $a_{1j}$  with  $x_j$ , and set  $a_{1j} = j$ ,  $1 \leq j \leq n$ .
- 4) Find the clique associated with  $x_1$  and  $y_2$ , say  $\{x_1, y_2, \dots, y_n\}$ . There is a unique matching between the  $x_i$ 's and the  $y_i$ 's.
- 5) Order the  $y_i$ 's such that  $x_i$  is connected to  $y_i$ , for  $2 \leq i \leq n$ .
- 6) Associate  $a_{j_1}$  with  $y_j$  and set  $a_{j_1} = j$ ,  $2 \leq j \leq n$ .
- 7) For each of the remaining  $(n-1)^2$  nodes of  $G$ , do the following, where  $W$  is a remaining node:
  - a) If  $W$  is connected to  $x_i$  then  $W$  is connected to a unique  $y_i$  and a unique  $x_j$ ,  $2 \leq i, j \leq n$ .  
Set  $a_{ij}$  to 1.
  - b) If  $W$  is not connected to  $x_i$ , then there exist

unique integers  $k$ ,  $i$ , and  $j$  such that  $W$  is connected to  $y_k, x_k, y_i$ , and  $y_j$ . Set  $a_{ij}$  to  $k$ .

Using Lemma 4 we get the following theorem.

Theorem 3: Latin square graph isomorphism is decidable in  $O(n^{\log_2 n} + O(1))$  steps.

### References

- 1) Denes, J. and Keedwell, A.D., Latin Squares and their Applications, Academic Press, New York, 1974.
- 2) Tarjan, R.E., private communication.
- 3) Lipton, R.J., Snyder, L., and Zalcstein, Y., "The Complexity of Word and Isomorphism Problems for Finite Groups."